A1 ICT Distribucija

Vabilo na LABYRINTH delavnico

Spoznali boste, zakaj je sistem za zaznavanje groženj z uporabo pasti eno izmed najučinkovitejših orodij za odkrivanje in zaustavitev napadalcev v omrežju podjetja.

A1 Slovenija,
Konferenčni center,
Ameriška 4, Ljubljana
20. november 2024

Naj napadalci raje tavajo po LABYRINTHU kot po vaših strežnikih

LABYRINTH

Univerza v Mariboru

hse

AT&T

PROPLUS

112 SOS

DELL

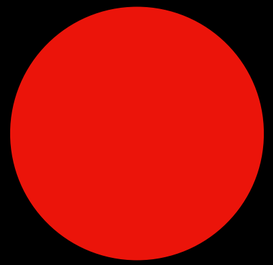
UNIVERZA V LJUBLJANI

BANK OF AMERICA

A1 ICT Distribucija

LABYRINTH

Kaj je tarča napadalcev?



Naj napadalci raje tavajo po LABYRINTHU kot po vaših strežnikih

Proces kibernetske varnosti

Metode zaznavanja

SIEM – Security Information and Event Management

EDR – Endpoint Detection and Response

NDR – Network Detection and Response

MDR – Managed Detection and Response

XDR – Extended Detection and Response

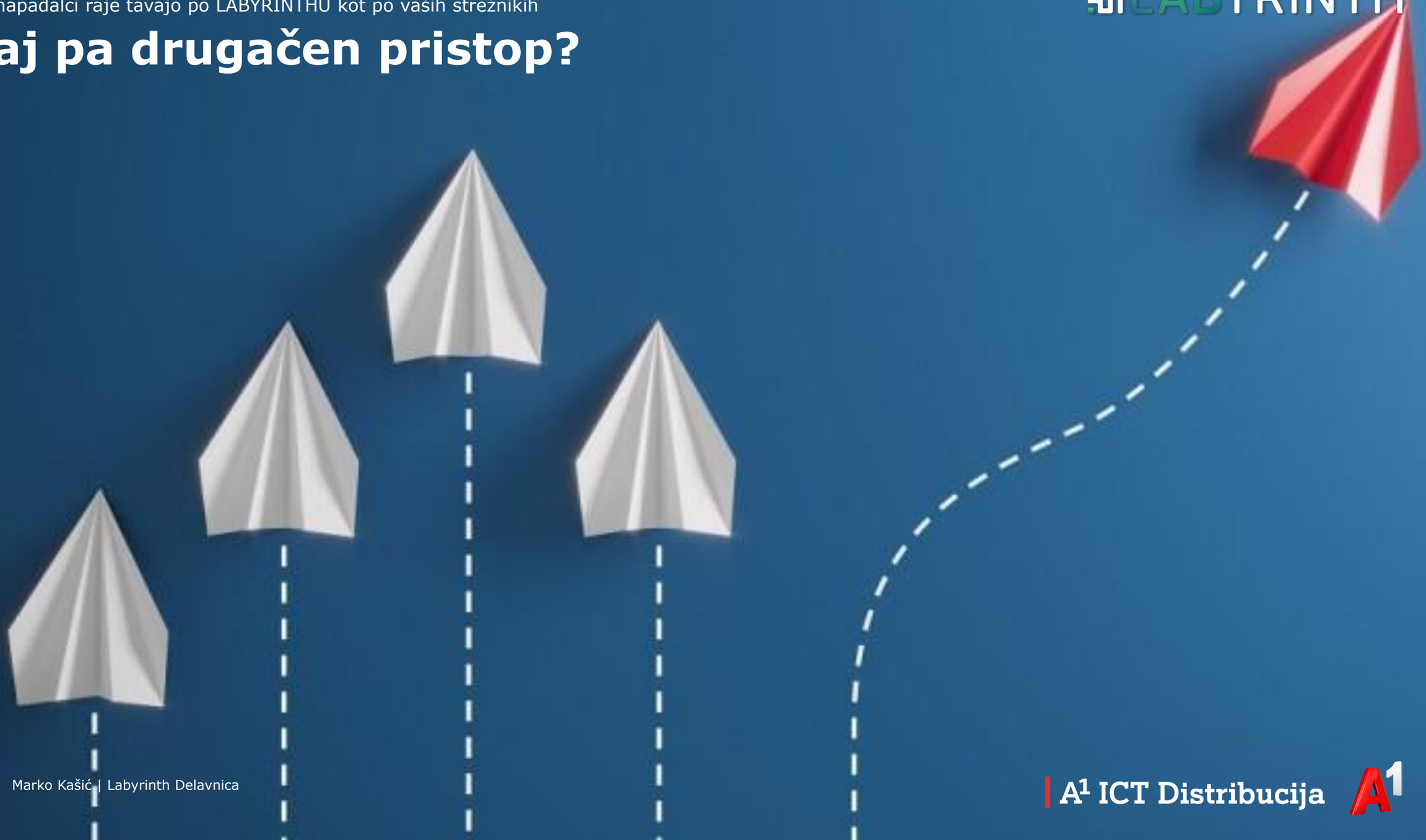
LABYRINTH

Metode zaznavanja

A1 ICT Distribucija

Naj napadalci raje tavajo po LABYRINTHU kot po vaših strežnikih

Kaj pa drugačen pristop?




IT'S A
TRAP

Platforma kibernetskega zavajanja

LABYRINTH

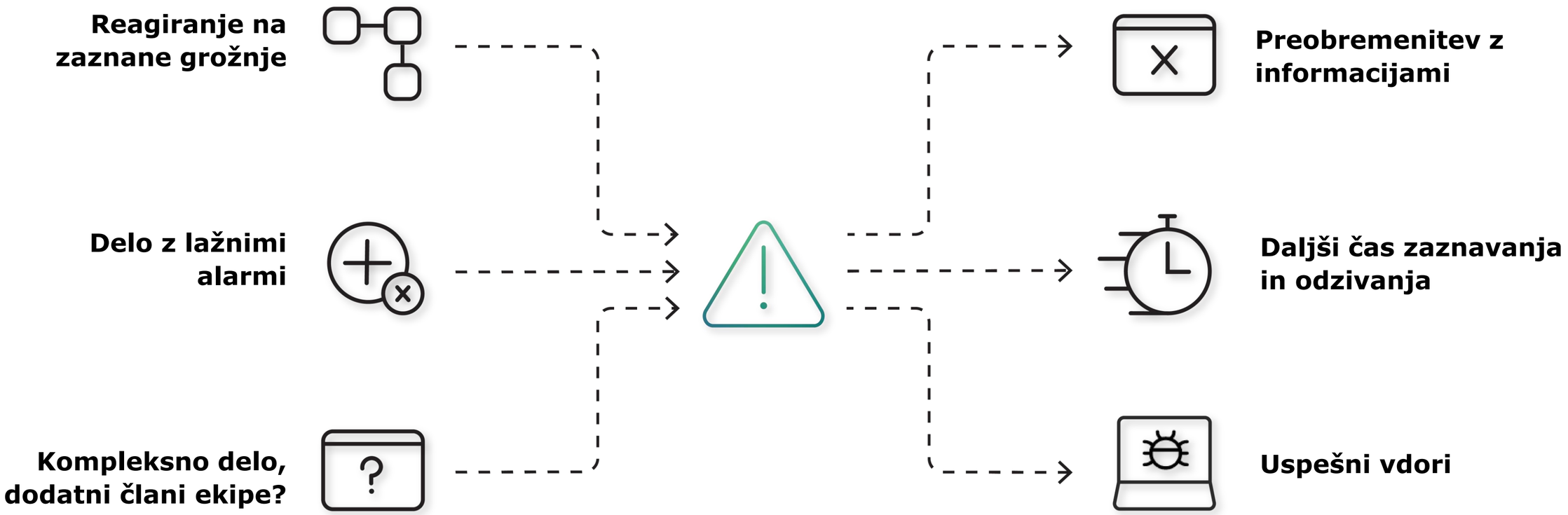
A1 ICT Distribucija

Kdo je Labyrinth?

- Ustanovljen 2019
- HQ – Zabrze, Poljska
- https://labyrinth.tech/

LABYRINTH

Izzivi



A1 ICT Distribucija

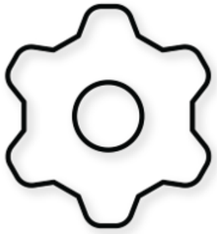
Zakaj Labyrinth

Zaustavitev naprednih groženj

Zaznava usmerjene in napredne napade pred predhodnega poznavanja oblike, tipa ali obnašanja grožnje.

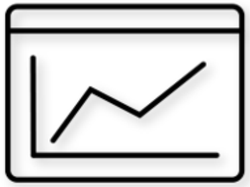
Brez vpliva na delovanje

Brez negativnega učinka na delovanje ostalih naprav v omrežju.



Enostavna implementacija

Hitra in enostavna implementacija brez sistemskih konfliktov in minimalnim vzdrževanjem: brez baz podatkov, podpisov ali pravil, ki jih je potrebno nastavljati ali posodabljati.



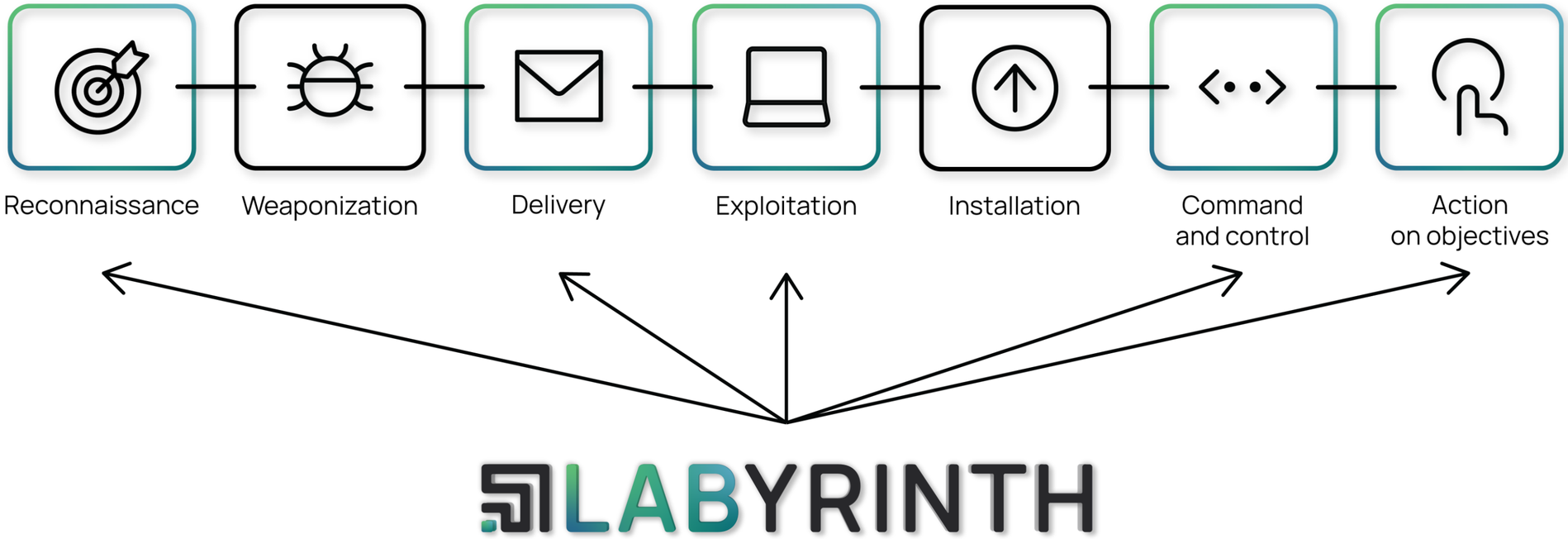
Znižanje operativnih stroškov*

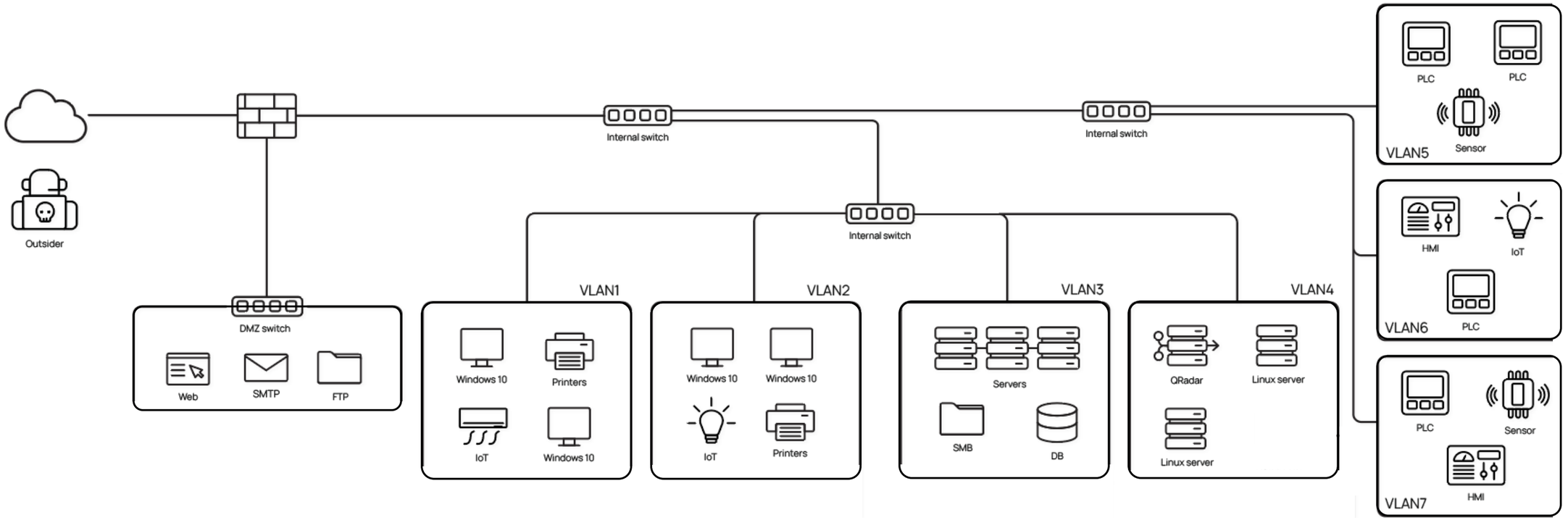
Ne zbira velikih količin podatkov, ne ustvarja lažnih alarmov, ne potrebuje specialističnega znanja za upravljanje.

* https://www.enterprisemanagement.com/news/press_release.php?p_id=2659

Kibernetski „kill-chain“

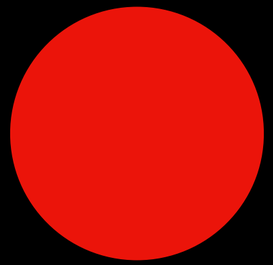
Labyrinth je najbolj učinkovit pri **zgodnjem zaznavanju napada**



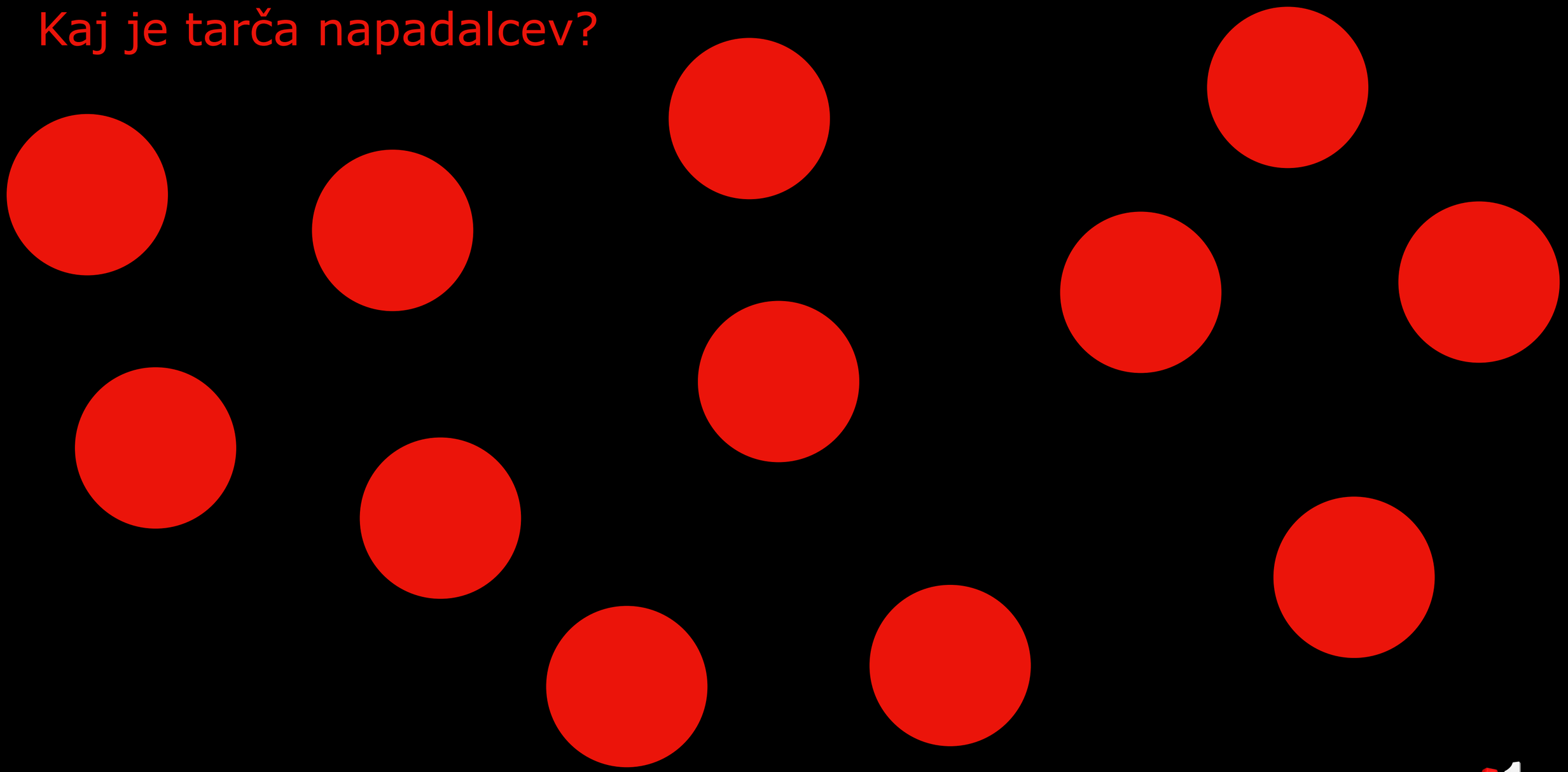

Outsider
Internal switch
Internal switch
Internal switch
DMZ switch
Web
SMTP
FTP
VLAN1
Windows 10
Printers
IoT
Windows 10
VLAN2
Windows 10
Windows 10
IoT
Printers
VLAN3
Servers
SMB
DB
VLAN4
QRadar
Linux server
Linux server
VLAN5
PLC
PLC
Sensor
VLAN6
HMI
IoT
PLC
VLAN7
PLC
Sensor
HMI

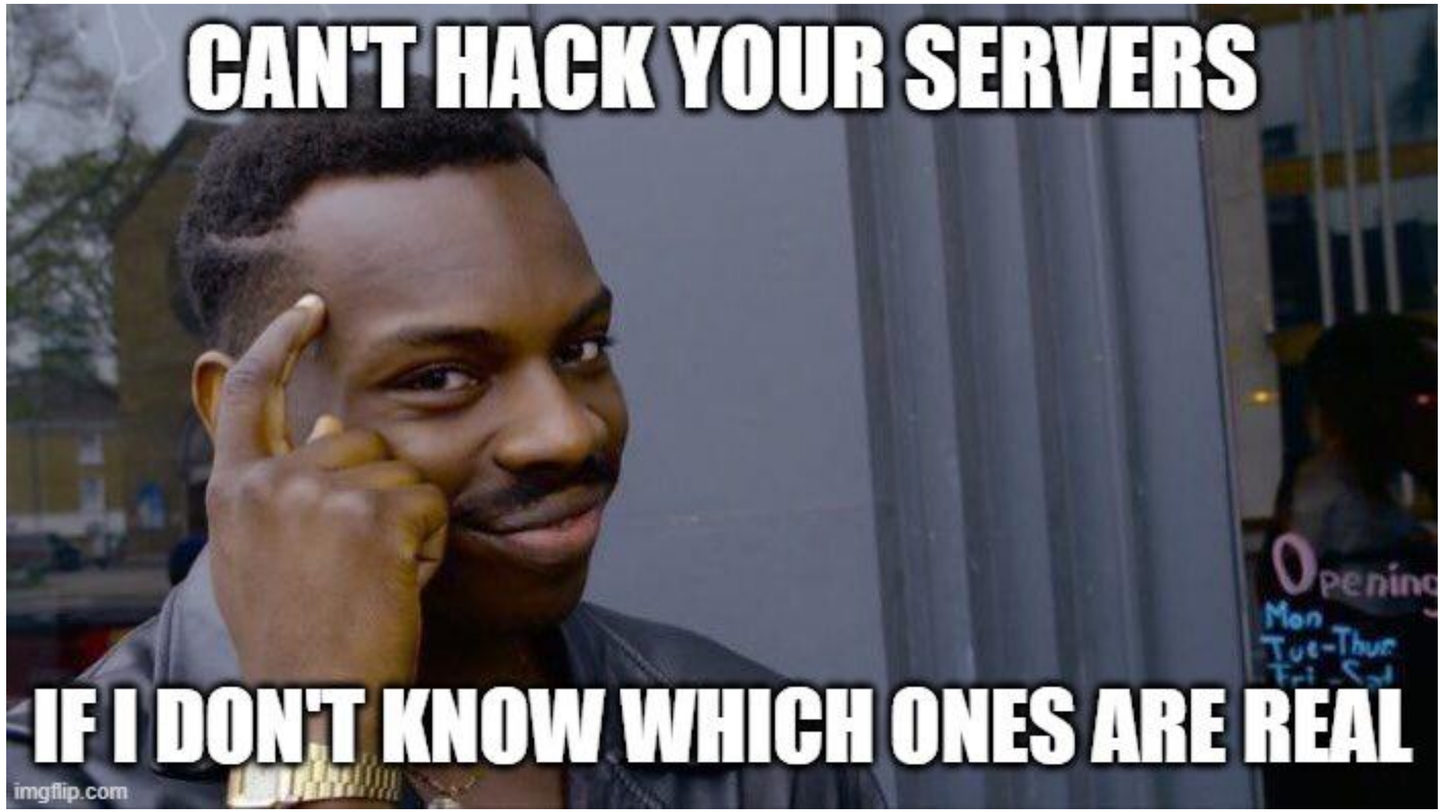
LABYRINTH

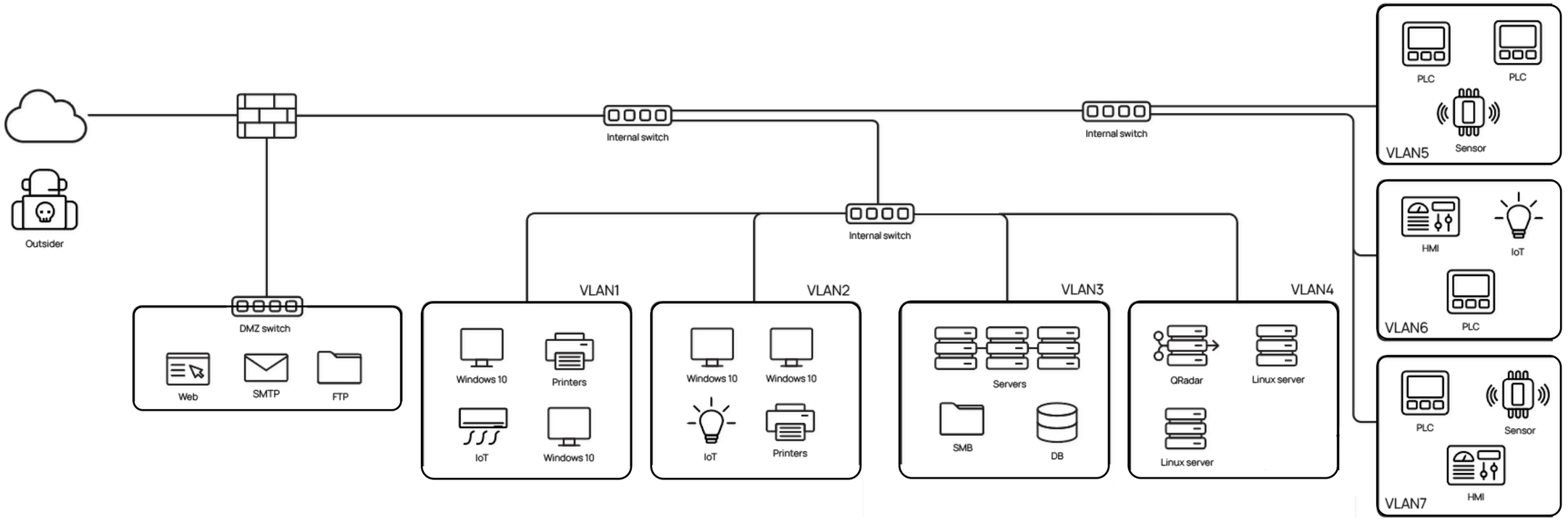
Kaj je tarča napadalcev?



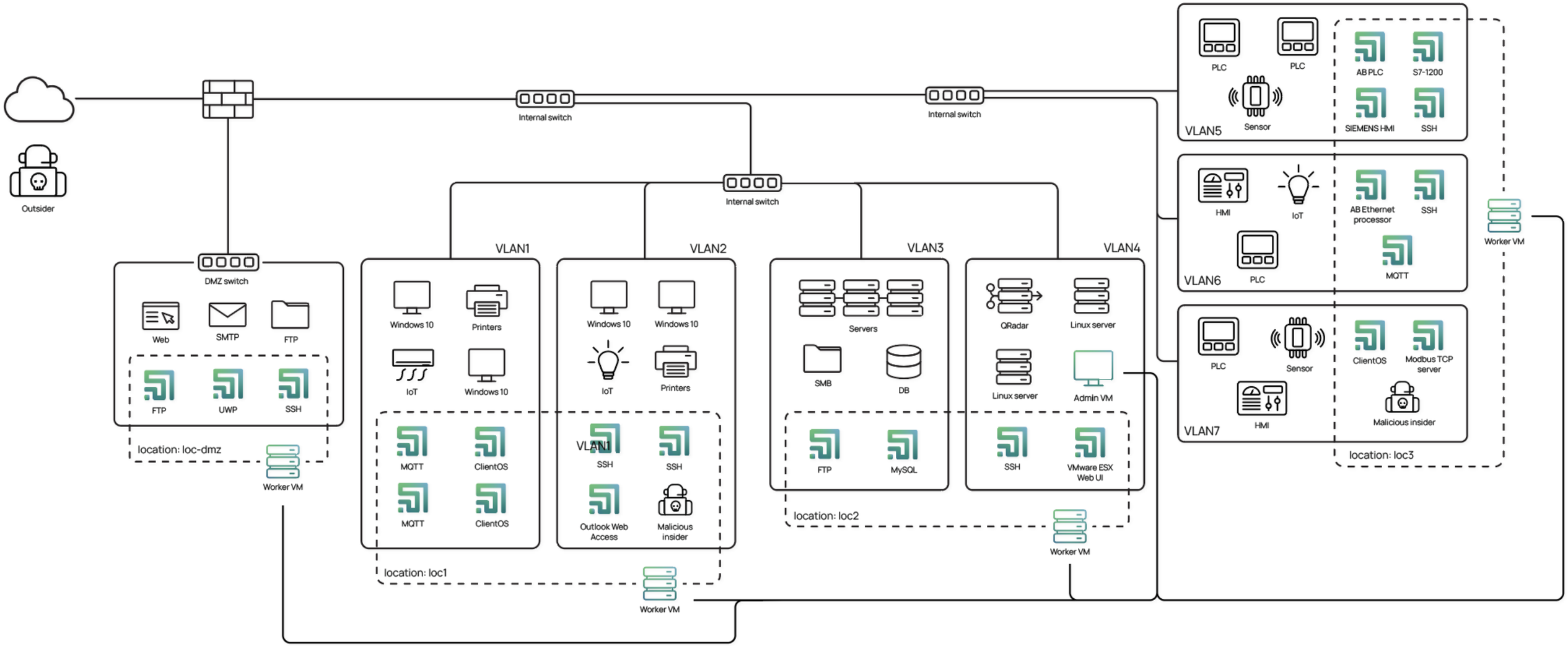
Kaj je tarča napadalcev?




CAN'T HACK YOUR SERVERS
IF I DON'T KNOW WHICH ONES ARE REAL
imgflip.com


Outsider
Internal switch
Internal switch
Internal switch
DMZ switch
Web
SMTP
FTP
VLAN1
Windows 10
Printers
IoT
Windows 10
VLAN2
Windows 10
Windows 10
IoT
Printers
VLAN3
Servers
SMB
DB
VLAN4
QRadar
Linux server
Linux server
VLAN5
PLC
PLC
Sensor
VLAN6
HMI
IoT
PLC
VLAN7
PLC
Sensor
HMI

LABYRINTH



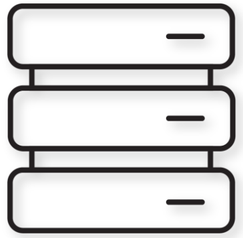
A1 ICT Distribucija

LABYRINTH

Gradniki platforme

Admin VM (Management Console)

All information collected at the Points is forwarded to the Management Console for incident analysis and response.



Worker VM

The Worker VM is the host that hosts all the Points in Labyrinth. It can operate in multiple VLANs simultaneously.

Point

Points simulate applications and services in a real-world IT environment and interact with attackers, keeping them inside the Labyrinth.

Host with Seeder Agent

Agents are deployed on real hosts and distribute attractive artifacts to them. The artifacts used by attackers direct them to Points.

LABYRINTH

VPRAŠANJA?

A1 ICT Distribucija

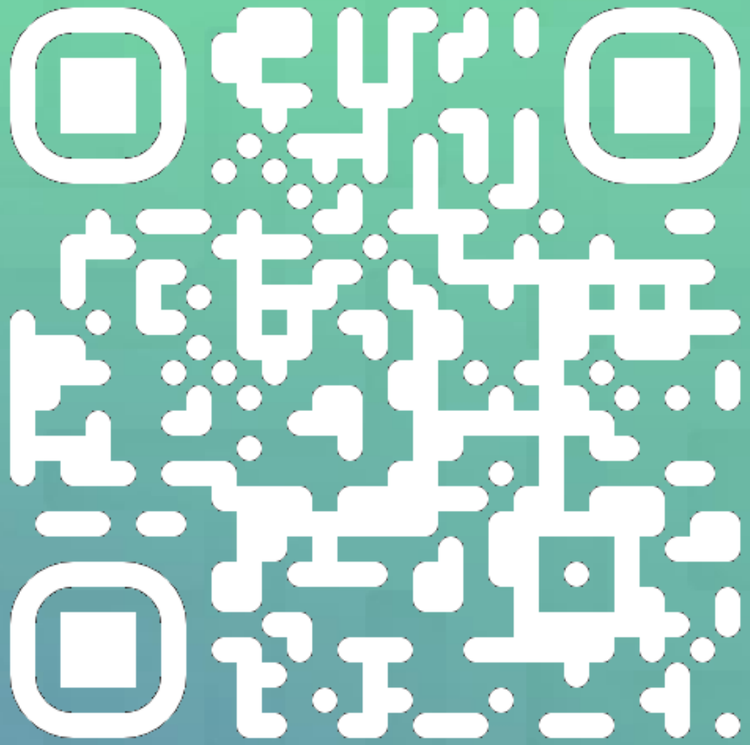
Naj napadalci raje tavajo po LABYRINTHU kot po vaših strežnikih

Zakaj Labyrinth?

- Hitra in enostavna **implementacija**
- **Brez vpliva** na aktivno infrastrukturo
- Brez **lažnih alarmov**
- Brezplačen **POC** (proof-of-concept)
- Pripravljeno za ponudnike storitev (**MSSP**)
- **Multi-tenant** opcije vgrajene

LABYRINTH

Več informacij



https://varnostne-resitve.si/

ict-partners@A1.si

Thank you

Marko Kašić

E marko.kasic@A1.si
M +386 40 440 842